



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1350  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,108	11/16/2001	Michael Burrows	200301735-2	2868

22879 7590 03/06/2006

HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS, CO 80527-2400

EXAMINER

CHAI, LONGBIT

ART UNIT PAPER NUMBER

2131

DATE MAILED: 03/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/991,108

Applicant(s)

BURROWS ET AL.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 05 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-40 and 42-63 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-40 and 42-63 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 1 – 58 have been presented for examination. Claim 41 has been cancelled and claims 1, 8, 22, 24, 25, 40, 44 have been amended; and new claims 59 – 63 have been added in an amendment filed 6/9/2005. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 40 and 42 – 63.

### ***Response to Arguments***

2. In response to Pre-Appeal Conference on request by Applicant for pre-appeal brief filed on 10/31/2005, a new ground of rejection has been made to withdraw the finality of the rejection. See the following office section.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 18 – 19, 37 – 38 and 42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per claim 18 – 19, 37 – 38 and 42, the claim limitation “determining if the information about he pattern of behavior is trustworthy” is not enabled by the

Art Unit: 2131

specification. Examiner notes this is because, according to the specification (Page 25, Line 17 – 19), the traffic monitor may use filters and configuration parameters to decide whether the information about the pattern of behavior it is receiving is likely to be trustworthy. However, the configuration parameters are not specifically disclosed in the specification at all and as such the invention of claim limitation is not clearly and concisely defined / specified in a manner which can be carried out by one skilled in the art to determine if the information about the pattern of behavior is trustworthy.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 7, 28 and 59 are rejected under 35 U.S.C. 102(e) as being anticipated by Gupta et al. (U.S. Patent 6389532).

As per claim 1 and 59, Gupta teaches a method for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

monitoring the network for any patterns of behavior (Gupta: Column 7 Line 28 – 38);

determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior (Gupta: Column 7 Line 28 – 38: denial of service attacks);

determining a proper action for mitigating that type of undesirable behavior, the proper action including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable (Gupta: Column 7 Line 39 – 47).

wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off at least one port of a forwarding device, filtering on Internet Protocol (IP) addresses, and filtering on media access control (MAC) addresses (Gupta: Column 7 Line 39 – 47).

As per claim 7 and 28, Gupta teaches the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets (Gupta: Column 7 Line 36 – 38: denial of service – i.e. too many packets directed to an overloaded server).

2. Claims 1, 7, 15, 17, 22, 28, 34, 36 and 59 are rejected under 35 U.S.C. 102(e) as being anticipated by Redlich (U.S. Patent 6591306).

As per claim 1, 22 and 59, Redlich teaches a method for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

monitoring the network for any patterns of behavior (Redlich: Column 18 Line 6 – 15: duplicate IP address);

determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior (Redlich: Column 18 Line 6 – 15);

determining a proper action for mitigating that type of undesirable behavior, the proper action including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable (Redlich: Column 18 Line 6 – 15).

wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off at least one port of a forwarding device, filtering on Internet Protocol (IP) addresses, and filtering on media access control (MAC) addresses (Redlich: Column 18 Line 6 – 15).

Art Unit: 2131

As per claim 7 and 28, Redlich teaches the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets (Redlich: Column 18 Line 6 – 15: a stolen Internet protocol (IP) address).

As per claim 15 and 34, Redlich teaches the undesirable pattern of behavior is too many ARP requests and wherein the monitoring includes verifying stability and lack of conflicts in an IP or MAC address mapping (Redlich: Column 18 Line 6 – 15).

As per claim 17 and 36, Redlich teaches the undesirable pattern of behavior is a simultaneous use of a network address, and wherein the proper action includes disabling any address associated to the network address that contradicts an address list in a network server or disabling any associated address that is not included in a list of addresses that are allowed to map to the network address (Redlich: Column 18 Line 6 – 15).

Art Unit: 2131

3. Claims 1, 2, 6, 8 – 14, 16, 20, 22, 23, 27, 29 – 33, 35, 39, 59 and 61 – 63 are rejected under 35 U.S.C. 102(e) as being anticipated by Bare (U.S. Patent 6389532).

As per claim 1, 22 and 59, Bare teaches a method for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

monitoring the network for any patterns of behavior (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7 and Column 12 Line 52 – 60);

determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior (Bare: Column 12 Line 52 – 60 and Column 4 Line 60 – 63);

determining a proper action for mitigating that type of undesirable behavior, the proper action including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable (Bare: Column 12 Line 56 – 60 and Column 4 Line 60 – 63).

wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off at least one port of a forwarding device, filtering on Internet Protocol (IP) addresses, and filtering on media access control (MAC) addresses (Bare: Column 12 Line 56 – 60 and Column 4 Line 60 – 63).



Art Unit: 2131

As per claim 61, Bare teaches a system comprising:

a network interface to a network (Bare: Figure 1); and

a packet traffic monitor to:

monitor the network for an undesirable behavior (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7 and Column 12 Line 52 – 60);

determine a type of the undesirable behavior (Bare: Column 12 Line 52 – 60 and Column 4 Line 60 – 63);

discover a topology of the network (Bare: Column 12 Line 56 – 60 and Column 4 Line 60 – 63); and

cause prevention of dissemination over the network of packets associated with the undesirable behavior based on the type of the undesirable behavior and topology of the network (Bare: Column 12 Line 56 – 60 and Column 4 Line 60 – 63).

As per claim 2 and 23, Bare teaches a discovery, including that of a network topology, facilitates the network monitoring and type of undesirable behavior determination (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7 and Column 12 Line 52 – 60).

As per claim 6 and 27, Bass teaches the undesirable pattern of behavior is any network pathology characterized as a broadcast storm or an address resolution protocol (ARP) fight (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7 and Column 12 Line 52 – 60).

As per claim 8 and 29, Bare teaches preventing the dissemination of the undesirable pattern of behavior includes discarding the packets associated with such behavior, isolating any of the computers at which such behavior originates, or isolating any network segments at which such behavior originates (Bare: Column 12 Line 56 – 60 and Column 4 Line 60 – 63).

As per claim 9, Bare teaches wherein the monitoring includes recovering a topology of the network using information obtained through a network management protocol interface (Bare: Column 4 Line 52 – 63).

As per claim 10, Bare does not disclose expressly the network management protocol is the simple network management protocol (SNMP). However, Official Notice is taken that the use of SNMP is one of the most widely used methods in the field for network management protocol.

As per claim 11 and 31, Bare teaches the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring includes learning a topology of the network from a forwarding database or table of a forwarding device in the network (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7, Column 4 Line 52 – 63 and Column 12 Line 52 – 60).

As per claim 12 and 33, Bare teaches the network is a shared data network (Bare: Figure 1).

As per claim 13, 14 and 32, Bare teaches the network is a switched Ethernet network and the forwarding device is a switch (Bare: Column 12 Line 52 – 60).

As per claim 16 and 35, Bare teaches teaches the proper action includes alerting a system administrator about the existence of the undesirable pattern of behavior (Bare: Column 58 Line 1 – 4).

As per claim 20 and 39, Bare teaches understanding the network topology facilitates disablement of ports in forwarding devices that connect to offending computers (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7, Column 4 Line 52 – 63 and Column 12 Line 52 – 60).

As per claim 30, claim 30 encompasses the similar scope as described in claim 9 and 10. Therefore, see same rationale addressed above in rejecting claim 9 and 10.

As per claim 62, Bare teaches the packet traffic monitor discovers the topology of the network by discovering that the network is one of a router-based network, a bridge-based network, and a switch-based network (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7, Column 4 Line 52 – 63 and Column 12 Line 52 – 60).

As per claim 63, Bare teaches the prevention of dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off a port of a

Art Unit: 2131

forwarding device, filtering on an Internet Protocol (IP) address, and filtering on a media access control (MAC) address (Bare: Column 4 Line 52 – 63).

4. Claim 42 is rejected under 35 U.S.C. 102(e) as being anticipated by Gupta et al. (U.S. Patent 6389532).

As per claim 42, Gupta teaches a system for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

one or more forwarding devices (Gupta: Column 6 Line 62 – 63); and

one or more packet traffic monitors each including:

means for monitoring the network for any patterns of behavior, including, if available, information about a pattern of behavior from any of the computers about another one of the computers (Gupta: Column 7 Line 28 – 38);

means for determining if the information about the pattern of behavior from any of the computers is trustworthy (Gupta: Column 7 Line 1 – 11).

means for determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior (Gupta: Column 7 Line 28 – 38);

means for determining a proper action for mitigating that type of undesirable behavior, the proper action, performed by mitigation means controlling the one or more forwarding devices, including preventing dissemination through the network of packets

Art Unit: 2131

associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior (Gupta: Column 7 Line 39 – 47).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent 6389532), in view of Bare (U.S. Patent 6389532).

As per claim 43, Gupta does not disclose expressly means for discovery, including that of the network topology, facilitates network monitoring and type of undesirable behavior determination.

Bare teaches a discovery, including that of a network topology, facilitates the network monitoring and type of undesirable behavior determination (Bare: Column 11 Line 42 – 44, Column 12 Line 5 – 7 and Column 12 Line 52 – 60).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bare within the system of Gupta because (a) Gupta teaches identifying the network undesirable behavior that may cause

Art Unit: 2131

network failures and (b) Bare teaches providing a mechanism for dynamically managing the topology of a data network to improve the network performance as well as eliminating loops that could lead to broadcast storms essentially crippling network performance and causing network failures (Bare: Column 4 Line 60 – 63).

6. Claims 3 – 4, 24 – 25 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bare (U.S. Patent 6389532), in view of Rodeheffer (U.S. Patent 5260945).

As per claim 3 and 24, Bare does not disclose expressly the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time.

Rodeheffer teaches the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time (Rodeheffer: see for example, Column 1 Line 42 – 48, Column 2 Line 9 – 45, Column 3 Line 21 – 26 and Column 7 Line 1 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rodeheffer within the system of Bare

because (a) Bare teaches identifying the network undesirable behavior that may cause network failures and (b) Rodeheffer teaches providing for an optimized recovery time period of network failures that can minimize the disruption time based upon the information records of failure recovery history (Rodeheffer: see for example, Column 1 Line 13 – 16 and Column 2 Line 34 – 45).

As per claim 4 and 25, Bare as modified teaches the time period corresponds to a skepticism level that depends on a history of the undesirable pattern of behavior, a skepticism level zero (0) denoting a good history (Rodeheffer: see for example, Column 3 Line 20 – 26 and Column 5 Line 62 – 67).

As per claim 60, Bare does not disclose expressly preventing the dissemination is performed for .a period of time, the method further comprising: lengthening the period of time as long as the undesirable behavior continues or intermittently reappears; and shortening the period of time in response to the undesirable behavior stopping for at least a predetermined time.

Rodeheffer teaches preventing the dissemination is performed for .a period of time, the method further comprising: lengthening the period of time as long as the undesirable behavior continues or intermittently reappears; and shortening the period of time in response to the undesirable behavior stopping for at least a predetermined time (Rodeheffer: see for example, Column 1 Line 42 – 48, Column 2 Line 9 – 45, Column 3 Line 21 – 26 and Column 7 Line 1 – 42).

See the same rationale of combination as addressed above in rejecting claim 3.

7. Claims 5, 26, 18 – 19 and 37 – 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bare (U.S. Patent 6389532), in view of Bass et al. (U.S. Patent 6185185).

As per claim 5 and 26, Bare does not disclose expressly the undesirable pattern of behavior is characterized in that it matches behavior defined by a network administrator as notable or undesirable.

Bass teaches the undesirable pattern of behavior is characterized in that it matches behavior defined by a network administrator as notable or undesirable (Bass: see for example, Column 3 Line 45).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bass within the system of Bare because (a) Bare teaches identifying the network undesirable behavior that may cause network failures and (b) Bass teaches an improvement mechanism in the prevention of broadcast traffic in computer networks (Bass: Column 2 Line 6 – 8).

As per claim 18 and 37, Bare does not disclose expressly if available from any one of the computers, the monitored pattern of behavior further includes information about a pattern of behavior by another one of the computers, the method further comprising: determining if the information about the pattern of behavior is trustworthy.



Art Unit: 2131

Bass teaches if available from any one of the computers, the monitored pattern of behavior further includes information about a pattern of behavior by another one of the computers, the method further comprising: determining if the information about the pattern of behavior is trustworthy (Bass: Column 2 Line 50 – 55). See the same rationale of combination as addressed above in rejecting claim 5.

As per claim 19 and 38, Bare as modified teaches filters and network configuration parameters are used in determining the trustworthiness (Bass: Column 2 Line 50 – 55).

8. Claims 21 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bare (U.S. Patent 6389532), in view of Rodeheffer (U.S. Patent 5260945), and in view of Singh (Patent Number: 6453430).

As per claim 21 and 40, Bare as modified teaches the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

However, Bare as modified does not disclose expressly the recovery time can be associated with an exponential recovery time interval.

Singh teaches the recovery time can be associated with an exponential recovery time interval (Singh: see for example, Column 4 Line 40 – 47).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Singh within the system of Bare as modified because Singh teaches providing significant advancements in fault management for recovery / restart sequence in a real-time or mission critical environments such as data communication networking devices or applications (Singh: see for example, Column 2 Line 32 – 39).

Accordingly, Bass as modified teaches the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

9. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent 6389532), in view of Singh (U.S. Patent 6453430), and in view of Rodeheffer (U.S. Patent 5260945).

As per claim 44, Gupta does not disclose expressly the dissemination through the network of packets associated with the undesirable behavior is prevented for a time

Art Unit: 2131

period that is exponentially exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

Singh teaches the recovery time can be associated with an exponential recovery time interval (Singh: see for example, Column 4 Line 40 – 47).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Singh within the system of Gupta because (a) Gupta teaches identifying the network undesirable behavior that may cause network failures and (b) Singh teaches providing significant advancements in failure management for recovery / restart sequence in a data communication networking environment (Singh: see for example, Column 2 Line 32 – 39).

Gupta as modified does not disclose expressly the recovery time is a time period that is exponentially exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

Rodeheffer teaches a recovery time period exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being shortened if the undesirable behavior stops for a predetermined time (Rodeheffer: see for example, Column 1 Line 42 – 48, Column 2 Line 9 – 45, Column 3 Line 21 – 26 and Column 7 Line 1 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rodeheffer within the system of Gupta

as modified because (a) Gupta teaches identifying the network undesirable behavior that may cause network failures (b) Rodeheffer teaches providing for an optimized recovery time period of network failures that can minimize the disruption time based upon the information records of failure recovery history (Rodeheffer: see for example, Column 1 Line 13 – 16 and Column 2 Line 34 – 45).

Accordingly, Gupta as modified teaches the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is exponentially exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

10. Claims 45 – 50, 52 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent 6389532), in view of Bass et al. (U.S. Patent 6185185).

As per claim 45, Gupta does not disclose expressly the packet traffic monitor is a separate device connected to the network and through the network to the one or more forwarding devices.

Bass teaches the packet traffic monitor is a separate device connected to the network and through the network to the one or more forwarding devices (Bass: see for example, Column 10 Line 29 and Column 4 Line 54).

Art Unit: 2131

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bass within the system of Bare because (a) Gupta teaches identifying the network undesirable behavior that may cause network failures (Gupta: Column 7 Line 35 – 38) and (b) Bass teaches an improvement mechanism in the prevention of broadcast traffic in computer networks (Bass: Column 2 Line 6 – 8).

As per claim 46 and 47, Gupta does not disclose expressly one or more of the computers have a dedicated built-in packet traffic monitor.

Bass teaches one or more of the computers have a dedicated built-in packet traffic monitor (Bass: see for example, Column 10 Line 20 –30). See the same rationale of combination as addressed above in rejecting claim 45.

As per claim 48, Gupta does not disclose expressly the network is a switched Ethernet network and forwarding devices are switches.

Bass teaches the network is a switched Ethernet network and forwarding devices are switches (Bass: see for example, Column 6 Line 27). See the same rationale of combination as addressed above in rejecting claim 45.

As per claim 49, Gupta does not disclose expressly the one or more forwarding devices include any combination of zero or more switches and routers.

Art Unit: 2131

Bass teaches the one or more forwarding devices include any combination of zero or more switches and routers (Bass: see for example, Column 10 Line 20 – 30). See the same rationale of combination as addressed above in rejecting claim 45.

As per claim 50, Gupta does not disclose expressly the network is a bridged network and the forwarding devices are bridges or smart bridges.

Bass teaches the network is a bridged network and the forwarding devices are bridges or smart bridges (Bass: see for example, Column 10 Line 28). See the same rationale of combination as addressed above in rejecting claim 45.

As per claim 52, Gupta does not disclose expressly the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a high-speed network segment.

Bass teaches the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a high-speed network segment (Bass: see for example, Column 6 Line 51). See the same rationale of combination as addressed above in rejecting claim 45.

As per claim 54, Gupta does not disclose expressly the one or more packet traffic monitors is implemented as a software module.

Bass teaches the one or more packet traffic monitors is implemented as a software module (Bass: see for example, Column 10 Line 20 – 30 and Column 4 Line 55 – 57). See the same rationale of combination as addressed above in rejecting claim 45.

11. Claims 51, 55 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent 6389532), and in view of Johnson (Patent Number: 5640504).

As per claim 51, Gupta does not disclose expressly the one or more packet traffic monitors are placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including one or more locations characterized as being next to an originator of the that behavior, at or next to each computer, at or next to each forwarding device or at the segment where the packets are to be monitored.

Johnson teaches the one or more packet traffic monitors are placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including one or more locations characterized as being next to an originator of the that behavior, at or next to each computer, at or next to each forwarding

Art Unit: 2131

device or at the segment where the packets are to be monitored (Johnson: see for example, Column 25 Line 10 – 17 and Column 3 Line 39 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Johnson within the system of Gupta because (a) Gupta teaches identifying the network undesirable behavior that may cause network failures (Gupta: Column 7 Line 35 – 38) and (b) Johnson teaches an effective distributed monitoring and control within a flexible network hierarchy (Johnson: see for example, Column 1 Line 5 – 9).

As per claim 55 and 56, Gupta does not disclose expressly the software module is a part of an operating system.

Johnson teaches the software module is a part of an operating system (Johnson: see for example, Column 25 Line 10 – 17 and Column 3 Line 39 – 42).

See the same rationale of combination as addressed above in rejecting claim 51.

12. Claims 53, 57 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent 6389532), and in view of Lewis (Patent Number: 6285748).

As per claim 53, Gupta does not disclose expressly the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of



Art Unit: 2131

undesirable behavior, the strategic locations including a place next to or at a network server.

Lewis teaches the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a place next to or at a network server (Lewis: see for example, Column 2 Line 28 – 34 and Figure 3).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Lewis within the system of Bass as modified because (a) Gupta teaches identifying the network undesirable behavior that may cause network failures (Gupta: Column 7 Line 35 – 38) and (b) Lewis teaches a network traffic monitor and control technique so that the network performance can be optimized (Lewis: see for example, Column 2 Line 27 – 34).

As per claim 57, Gupta does not disclose expressly the one or more packet traffic monitors co-operate with one another in the discovery of the patterns of behavior.

Lewis teaches the one or more packet traffic monitors co-operate with one another in the discovery of the patterns of behavior (Lewis: see for example, Column 6 Line 35 – 48 and Column 8 Line 1 – 20).

See the same rationale of combination as addressed above in rejecting claim 53.

Art Unit: 2131

As per claim 58, Gupta does not disclose expressly the one or more packet traffic monitors are configured to sample points on the network randomly or selectively rather than sampling the entire network.

Lewis teaches the one or more packet traffic monitors are configured to sample points on the network randomly or selectively rather than sampling the entire network (Lewis: see for example, Figure 3).

See the same rationale of combination as addressed above in rejecting claim 53.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

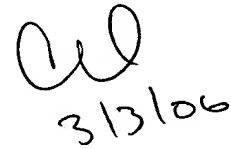
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai  
Examiner  
Art Unit 2131

LBC



CHRISTOPHER REVAK  
PRIMARY EXAMINER



3/3/06